

REMARKS

The Examiner is thanked for the performance of a thorough search.

Claims 1-29 are under examination.

Claims 1-7, 11-15, 17-19, and 22-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dougall et al. (Dougall, Pub.No. 2003/0093485 A1) in view of Quick, Jr. (Quick, Patent No.: US 6,260,147 B1). The rejection is respectfully traversed for the following reasons.

I

Claim 1 recites, in part:

selecting a subset from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol (emphasis added).

Contrary to the rejection's assertion, Dougall fails to teach or suggest these limitations. Furthermore, Applicants assert that Quick does not teach or suggest these limitations, while noting that the rejection does not assert that Quick teaches or suggests these limitations. Therefore, the combination of Dougall and Quick fails to teach or suggest these claim limitations.

Dougall does not teach or suggest selecting a subset from a set of data in a particular payload, as claimed. Dougall teaches transferring a packet (FIG. 20) with a payload 920 that may or may not be encrypted. However, there is no teaching or suggestion in Dougall of selecting a subset of the particular payload. Thus, Dougall fails to teach or suggest selecting a subset from a set of data to be communicated between the client and the server in a particular payload, as claimed.

For the foregoing reasons, the combination of Dougall and Quick fails to teach or suggest the recited limitations, “selecting a subset from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol,” as claimed.

II

Claim 1 further recites, in part:

determining a secret integer that is unique for the subset among a plurality of subsets
in a plurality of payloads.

The rejection concedes that Dougall fails to teach the above claim limitations. Applicants assert that Dougall does not teach or suggest these claim limitations. Moreover, contrary to the rejection’s assertion, Quick fails to teach or suggest these limitations. Therefore, the combination of Dougall and Quick fails to teach or suggest these claim limitations.

Quick teaches (col. 3, lines 1-6) that a subscriber enters a user identifier and a password into a terminal when the subscriber wishes to register a terminal to his subscription. Responsive to the subscriber input, the terminal generates a public/private key pair and stores it. The rejection appears to assert that the user password corresponds to the claimed secret integer. Applicants disagree. The claimed secret integer is unique for the subset among a plurality of subsets in a plurality of payloads. Thus, Claim 1 implies that a different integer is used for different subsets in the plurality of payloads. Quick teaches that the user identifier and password are used

to register a terminal to the user's subscription. Quick does not teach or suggest that the password is unique for any subset among a plurality of subsets in a plurality of payloads, as claimed. Rather, Applicants assume that because the password is used to register a terminal to a subscription that the same password would be used for different payloads associated with the terminal and have found no teaching or suggestion in Quick to the contrary. Further, the user identifier (col. 3, line 2) is neither taught nor suggested by Quick to be unique for the subset, as claimed.

The rejection also appears to assert that Quick discloses a session key that teaches the claimed secret integer. A session key is used for an entire session, which may comprise multiple payloads. Therefore, the same session key may be used for different payloads. Thus, the session key is not unique for the subset among a plurality of subsets in a plurality of payloads, as claimed.

For the foregoing reasons, the combination of Dougall and Quick fails to teach or suggest the recited limitations, "determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads."

III

Claim 1 further recites, in part:

sending, from a sending device of the client and the server to a receiving device of the client and the server, in the particular payload, the encrypted data and clue information to determine, only at the client and the server, the secret integer for decrypting the encrypted data (emphasis added).

The combination of Dougall and Quick fails to teach or suggest these claim limitations. Applicants note that, as previously discussed, the secret integer is recited as being unique for the subset among a plurality of subsets in a plurality of payloads. Thus, in the context of Claim 1 as a whole, the recited clue information is used to determine a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads.

While Dougall may teach sending a key index and a program identifier in a packet (FIG. 20), the key index and program identifier are not used to determine a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads, as Claim 1 taken its entirety implies. Dougall teaches sending a packet (FIG. 20), which contains a key index 917 that is used along with a program ID 918 to index the correct decryption key stored at the client node. There is no teaching or suggestion in Dougall that the decryption key stored at the client node is unique for the subset among a plurality of subsets in a plurality of payloads, as Claim 1. Applicants note that Dougall teaches that the program identifier is unique to the program whose contents are carried by the packet [0137]. However, Dougall does not explicitly teach that the decryption key that results from using the programming identifier and the key index is unique to the subset among a plurality of subsets in a plurality of payloads.

Moreover, it is not inherent in Dougall that the decryption key that results at the client node from using the transferred programming identifier and the key index is unique to the subset among a plurality of subsets in a plurality of payloads, as claimed. For a disclosure to inherently teach a claim limitation the limitation must necessarily be present. It is not necessarily true that a combination of a unique program identifier with a key index will produce a unique value. For example, it is entirely possible that different program identifiers

combined with different key indexes can index to the same description key. Therefore, Dougall does not inherently teach the limitations of Claim 1.

Furthermore, neither the program identifier nor the key index, which Dougall teaches are sent in the clear in the packet, can be the claimed secret integer, as the claimed secret integer is only determinable at the client and the server, which implies that the secret integer is not sent in the clear in the packet.

Thus, Dougall does not teach or suggest sending clue information to determine, only at the client and the server, the secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads, as claimed.

Quick does not remedy this deficiency in Dougall in that the teachings of Quick combined with Dougall do not teach or suggest these limitations. As previously discussed, Quick does not teach or suggest determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads, as claimed. Therefore, Quick does not remedy the deficiency in Dougall of the decryption key (that the rejection asserts as being the claimed secret integer) not being a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads, as claimed.

Independent Claims 24, 26 and 28 recite similar limitations to those discussed in the response to Claim 1. For at least the reasons discussed in the response to Claim 1, Claims 24, 26 and 28 are patentable.

Claims 2-7, and 11-13 depend from Independent Claim 1, incorporating limitations therefrom. As explained above, Claim 1 includes limitations that define patentable subject

matter. Therefore, these dependant claims recite patentable subject matter for at least the same reasons Claim 1 recites patentable subject matter.

Independent Claim 14 recites, in part:

receiving, at a receiving device of the client and the server from a sending device of the client and the server, in a particular payload of the unencrypted transfer protocol, encrypted data and clue information to determine, only at the client and the server, a secret integer unique for the encrypted data in the particular payload among a plurality of subsets in a plurality of payloads.

The rejection asserts that Dougall teaches the above limitations. However, as discussed in part II herein, Dougall fails to teach or suggest, “a secret integer unique for the encrypted data in the particular payload among a plurality of subsets in a plurality of payloads,” as claimed. Moreover, for at least the reasons discussed in part II in the response to Claim 1, the combination of Dougall and Quick fails to teach or suggest these claim limitations.

Furthermore, for at least reasons discussed in parts III in the response to Claim 1, the combination of Dougall and Quick fails to teach or suggest the above claim limitations.

Independent Claims 25, 27 and 29 recite similar limitations to those discussed in the response to Claim 14. For at least the reasons discussed in the response to Claim 14, Claims 25, 27 and 29 are patentable.

Claims 15, 17-19 and 22-23 depend from Independent Claim 14, incorporating limitations therefrom. As explained above, Claim 14 includes limitations that define patentable subject matter. Therefore, these dependant claims recite patentable subject matter for at least the same reasons Claim 14 recites patentable subject matter.

Claims 8-10, 16, and 20-21 were rejected under 35 U.S.C. 103(a) as being unpatentable over Dougall, in view of Quick, in further view of Carman et al. U.S. Published Patent Application No. 2002/0199102 (“Carman”).

Claims 8-10, 16 and 20-21 depend from Independent Claim 1 or Independent Claim 14, incorporating limitations therefrom. As explained above, these independent claims include limitations that define patentable subject matter over Dougall and Quick. Carmen is used as allegedly teaching applying a hash function and as allegedly teaching determining a shared secret key based on clue information. However, Carmen is not alleged to nor does Carmen remedy the deficiencies of Dougall and Quick discussed herein. Therefore, Independent Claims 1 and 14, along with claims dependent therefrom, are allowable over the combination of Dougall, Quick, and Carmen.

Dougall is not a valid reference under 35 U.S.C. 103

Applicants further traverse the rejection to Claims 1-29 on the grounds that Dougall is not a valid reference under 35 U.S.C. 103. Dougall has a filing date of May 15, 2002. The present application has a filing date of February 28, 2002, which is prior to the filing date of Dougall. Applicants are aware that Dougall may be a continuation of U.S. application No. 09/950,927, filed on Sep. 12, 2001. However, upon careful review of versions of Dougall that

are publicly available (e.g., a version on the USPTO public website on August 31, 2005), the Applicants have found no specific reference in Dougall claiming priority to the earlier filed application. Hence, Dougall is not entitled to benefit from the filing date of the prior application.

Under 35 U.S.C. 120, in order for a patent application to benefit from an earlier filing date in the United States, the application must contain, or be amended to contain, a specific reference to the earlier filed application. Applicants have found no such reference in any published version of the Dougall application of which Applicants are aware. If the Examiner is aware of information indicating that the Dougall application properly claims benefit under 35 U.S.C. 120 to an application having a filing date prior to the filing date of the present application, the Examiner is requested to provide such information to the Applicants. For the foregoing reasons, based on publicly available versions of the Dougall Application known to Applicants, Dougall's effective filing date is May 15, 2002, which is after the filing date of the present application.

Because no claim in the present application is rejected without reference to Dougall, Applicants asserts that all claims are allowable over the cited art.

CONCLUSION

The Applicants believe that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

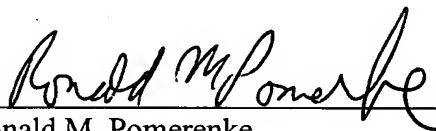
To the extent necessary to make this reply timely filed, the Applicants petition for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Date: August 31, 2005



Ronald M. Pomeroy
Reg. No. 43,009

2055 Gateway Place, #550
San Jose, CA 95110
Telephone: (408) 414-1080, ext. 210
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop AMENDMENT
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on

8/31/05

by



Trudy Bagdon